Information Technology Security and Privacy Policy

July 2002

1 INTRODUCTION

1.1 Purpose

FSA's Information Security and Privacy policies reflect management's decisions, intentions, definitions, and rules on information security and protection of private information. These policies set the minimum level of security required at FSA and establish the criteria against which we measure our results. These FSA Information Security and Privacy policies provide the foundation for various information security guidelines, standards, processes and procedures.[1]

1.2 Scope

Information security involves the organizational, technical and management measures necessary to safeguard information assets against unauthorized access, disclosure, duplication, denial of use, modification, diversion, destruction, loss, theft, or misuse – whether malicious or accidental. Information security jurisdiction covers all information assets (property of the U.S. Government), beginning with the electronic or manual input of data and ending upon the transfer of responsibility to non-FSA or FSA contractor employee or facility. . These policies address Information Security requirements exclusively for FSA assets, personnel, facilities, and contracted resources. Department of Education IT resources (including EDNET and its components) are addressed by the Department's Information Security Guide, and are outside the scope of FSA Information Security policies.

1.3 FSA Security Fundamentals

FSA systems must protect the confidentiality, integrity and availability of all information assets. The following high-level fundamentals provide the basis for all information security activities. These principles are simple, broad statements that form a "Constitution" for information security that are tailored to the needs of FSA:

- **Individual Accountability**
  Each individual is responsible for his or her actions in safeguarding FSA information assets.
- **Need-to-Know and Need-to-Do (Least Privilege)**
  Each individual is authorized access to only those FSA information assets required to perform his or her job.
- **Separation of Duties and Functions**
  - Operation/Production No single individual may have exclusive control over a particular FSA information asset or process, ensured by a real and lasting separation of security authority and responsibility in all FSA programs and operations.

[1] The guidelines, standards, processes, and implementation procedures can be found on connectEd and FSANet

- Development To ensure stability of FSA computing environment, there should be a separation of duties among development, testing and production tasks.

- **Principle of Proportionality**
  Information security and privacy measures will be implemented in reasonable proportion to the identified risks they are designed to protect against and the business value of the assets they protect.
- **Maintenance of Trust**
  FSA systems must be developed as systems worthy of trust. The adequacy of the security and privacy protections shall be judged at least in part by how FSA's customers and partners view the protection provided.
- **Security and Privacy by Design**
  FSA security is developed as part of a Solution Life Cycle process. From the initial concept to retirement, FSA integrates security controls into its systems and applications. All security solutions must integrate into an overall strategic security architecture.

All FSA policies, guidelines, and standards and practices must be consistent with these principles.

1.4 Compliance

Compliance with Information Security Policies is mandatory. If an individual (a Federal employee or contractor) violates the provisions in this policy, either by negligence or intent, FSA may take appropriate disciplinary action in accordance with Departmental standards of conduct, a system's rules of behavior, contract provisions, or the Departments disciplinary or termination policies.

1.5 Exceptions

Any exceptions to any portion of this policy as a result of a risk-based decision must be approved in writing by the system owner, and may require higher-level management authorization. The FSA Computer Security Officer (CSO) must be notified in writing of all exceptions to these policies.

1.6 Applicability

This policy applies to all FSA operations. FSA employees, consultants, contractors, interns, temporary employees, or other third parties accessing FSA information assets are subject to this policy, and have the same responsibilities as FSA employees.

Partner organizations, such as schools, lenders, guarantors and servicers, and their employees have parallel responsibilities for security and privacy which are set forth in various program participation agreements and contracts. However, FSA has ultimate responsibility for protecting student aid data, so FSA must manage this syndicated risk vigorously and systematically.

This policy also applies after termination of employment with FSA.

1.7 Policy Document Administration

The FSA Security and Privacy Team will review Information Security Policies as often as necessary but no less than annually. Additional policies may be issued as the need arises, and will be incorporated into the Information Technology Security and Privacy Policy document.

1.8 References

This document is based on standards contained in the following documents:

- NIST 800-18, Guide for Developing Security for IT Systems
- NIST Special Publication 800-26, Self-Assessment Guide for Information Technology Systems[2]
- International Standard – Information Technology – Code of Practice for Information Security Management 17799:2000
- U.S. Dept of Education Information Technology Security Policy
- The Privacy Act of 1974
- The Government Information Security Reform Act (GISRA)

These documents provide a comprehensive set of baseline policies comprising federal and international best practices in information security and privacy. Strategies
FSA information security and privacy strategies are long-term directions that serve as the basis for adequate planning and security solutions to meet FSA business needs now and in the future.

FSA information security is multi-dimensional. To be effective, information security requires constant review of the following strategies:

- Information security tools, methods, and practices will not rely on secrecy or obscurity to be effective.
- Information security decisions will be based on risk analyses and assessment methods that include – to the extent possible – metrics that capture the short and long-term business value of alternatives.
- Information security will include periodic reviews of the business value of security measures already in place.

1.9 Security and Privacy Organization

All those who use FSA information assets are implicitly part of the FSA security and privacy organization. This resulting virtual organization must make sure security policies are in place and managed accordingly. Effective management of FSA information requires that everyone who has access to FSA information assets:

- Understands security roles and responsibilities.

[2] 800-26 includes requirements from OMB A-130 Appendix III, FISCAM, and Computer Security Act.

- Manages risks so appropriate measures can be taken to protect the confidentiality, integrity and availability of FSA information assets.
- Participates in awareness programs to make sure security policies are communicated and understood.
- Reports security incidents, violations, and known vulnerabilities to management and to FSA's Security and Privacy team.
- Makes sure that the outsourcing of information services to a third-party service provider does not introduce degradation of information security beyond that accepted as a business risk.

1.10 Roles and Responsibilities

FSA assigns security and privacy responsibilities to numerous individuals, with ultimate responsibility for these matters assigned to the Chief Operating Officer (COO). A security responsibility assigned to a specific position may be delegated or reassigned to another position. FSA's primary objective is to make sure an identified individual or group performs all security functions. The COO delegates much of his/her operational security responsibilities to the business channel leads, or Functional Managers (FM). A Functional Manager has budgetary and operational control of the systems within his/her business channel. The Functional Manager appoints a System Manager in writing. Each Functional Manager relies upon System Managers (SM) to oversee and manage the security of individual systems. The System Manager appoints, in writing, a System Security Officer (SSO) to manage the administrative details of system security, including the system's documentation, personnel clearances, and interaction with contractor support security professionals.

The FSA Office of the Chief Information Officer (O/CIO), in addition to managing several FSA systems, writes Information Security Policies, standards, and guidelines, provides security awareness and training to FSA employees and contractors, and responds to security matters presented by FSA channel personnel. The FSA CIO delegates much of this responsibility to the Computer Security Officer (CSO). The CSO manages the FSA security and privacy program and actively supports the business channels in the development and maintenance of systems worthy of trust.

1.11 Document Structure

In addition to this Introduction, this policy document is divided into three sections:

2.0 Enterprise Management Controls,
3.0 System Operational Controls, and
4.0 System Technical Controls.

This document's format follows the outline of NIST Special Publication 800-18, Guide for Developing Security Plans for Information Systems. Formatting the policy in this way is intended to aid policy implementation in FSA System Security Plans.

2 ENTERPRISE MANAGEMENT CONTROLS

The Enterprise Management Controls section outlines security topics that are normally addressed by management in the organization's information security program. In general, these controls focus on the management of the information security program and the management of risk within the organization. The types of control measures must be consistent with the need for protecting the general support system, major application or application.

System Managers are responsible for implementing risk-based, cost effective policies, based upon business-type decisions. Procedures based on these policies provide security protection for information collected or maintained on the information systems for which they are responsible.

2.1 Risk Management

The information processed by each FSA system must be analyzed to determine its level of sensitivity. The analysis will consider the criticality of the system to FSA's business processes and the impact on critical FSA functions if the confidentiality, integrity and/or availability of the system and the data it contains were compromised.

The sensitivity analysis must contain both a general description of sensitivity and a list of applicable laws, regulations, and policies that establish specific requirements for confidentiality, integrity, and availability of data/information in the system. It should also indicate if the information's sensitivity level is high, medium, or low for each of the three categories. If the system processes information subject to the Privacy Act, the SSO must document the number and title of the Privacy Act system of records in the system's security plan and whether the systems are used for computer matching activities.

FSA systems must practice information security throughout their entire life cycle. Each FSA System Manager must budget for and oversee the completion of risk assessments for all Information Technology (IT) systems under his/her control. These assessments must be updated every three years at a minimum by an independent evaluator, or whenever a major change[3] to the system occurs. Each assessment must include the name of the assessor and the date the assessment was completed. In partnership with channel leadership, the System Manager must:

- Supervise an assessment of the risk to each IT system for which he/she is responsible that considers internal and external threats to the confidentiality, integrity and availability of the system and to data supporting FSA's business operations.
- Determine the effectiveness of any countermeasures or risk mitigations for the system(s) being assessed and whether they are adequate.
- Supervise a mission/business impact analysis to determine potential effects of unmitigated risks on the mission or business process the IT system supports, to

[3] See NIST Special Publication 800-18 for a definition of a major change.

include an estimated degree of harm or loss that could occur if corrective actions are not taken.

- On the basis of the impact analysis, recommend corrective or mitigating actions to bring the system risk to a level the program official is willing to accept.
- Propose an implementation schedule and milestones with cost estimates for mitigating unacceptable risks.
- Monitor updates of a system's security plan with new procedures.
- Maintain a list of known system vulnerabilities, system flaws, or weaknesses, that could be exploited by the threat source, including those accepted as risk based decisions.

The SSO must maintain on file the risk assessment reports and related management approvals.

2.2 Security Control Reviews

System Managers are responsible for periodic management testing and evaluation of the effectiveness of security control policies, procedures and techniques, and for remediation of any noted deficiencies found during these tests. Security controls of the FSA system and any connected system must be consistent with, and an integral part of, the FSA IT architecture.

Every FSA system must also undergo tests and examinations, (i.e. network scans, penetration testing) of key controls on a routine basis. If security incidents or significant weaknesses are found, FSA must take remedial or corrective actions and report them to FSA management.

FSA System Managers must budget for and conduct a routine self-assessment, in NIST 800-26 format, every three years or whenever a major change occurs. Additionally the Inspector General or another independent evaluator may conduct an independent review. The findings from these reviews will be reported to OMB as required by the Government Information Security Reform Act (GISRA). FSA must take any system review seriously and dedicate adequate resources to appropriately address the deficiencies reported in the review. Similar to the requirement in risk management, FSA System Managers must aggressively implement appropriate actions to mitigate any findings in order to bring the system risk to a level the System Manager is willing to accept.

2.3 System Security Plan

Every FSA System Manager must have an approved system security plan written in the format and containing the topics prescribed in NIST Special Publication 800-18. The system security plan must describe the system and its relationship with all interconnected systems. The system security plan must contain synopses of supporting documents (i.e. Disaster Recover Plan, Configuration Management Plan, etc,) and, although not required, may contain these supporting documents as appendices. The SSO must review and update the security plan at least annually to reflect current conditions and risks. Security plans must be dated to ease tracking of modifications and approvals, and a summary of the plan must be incorporated into the strategic IT Blueprint of FSA.

2.4 Rules of Behavior

FSA managers must establish a written Rules of Behavior for each FSA system. Rules of Behavior reflect administrative as well as technical security controls. They also delineate responsibilities, detail the expected behavior of all individuals with access to the system and define penalties for their violation. The Rules of Behavior must be published, distributed, and signed by every developer, maintainer, and user of the system. The set of rules must describe the use of, and access to, FSA systems and set appropriate limits on any interconnected equipment that permits access to them. The Rules of Behavior must contain procedures for friendly and unfriendly termination of employment.

FSA managers must differentiate between:

- Rules that must always be enforced versus rules that are conditional or optional, and
- Guidelines that express what are forbidden unless expressly authorized versus what is permitted unless expressly forbidden.

The Rules of Behavior must include, but are not limited to, such actions as:

- Work at home,
- Protection of Privacy Act information,
- Reporting violations,
- Dial-in access,
- Consent to monitoring,
- Connection to the Internet,
- Use of copyrighted works,
- Limitations on the unofficial use of government equipment,
- The assignment and limitation of system privileges,
- Individual accountability, and
- Consequences for violating the rules of behavior.

2.5 Solution Life Cycle

Every FSA system must follow the FSA Security Process Guide[4]maintained by the FSA Security and Privacy team. The Security Process Guide is divided into six phases:

1. Vision
2. Definition
3. Construction
4. Deployment
5. Support
6. Retirement

Each phase of the lifecycle contains a corresponding security requirements checklist to be completed at the conclusion of each phase by the System Security Officer (SSO). No

[4] The FSA Security Process Guide is located as an appendix in FSA Solution Lifecycle.

system may proceed to the next lifecycle phase until the security checklist is complete and signed by the SSO and SM.

2.6 Certification and Accreditation (Awaiting ED guidance)

All FSA systems must perform Certification and Accreditation before becoming operational unless the system receives an Interim Authority To Operate (IATO). The system's owner may obtain an IATO for a period not to exceed 6 months when the system has the following:

- A full Risk Assessment;
- A draft Security Plan, and
- A Project Plan for full accreditation.

2.7 Security and Privacy Awareness and Training

All FSA employees are responsible for the confidentiality, integrity and availability of FSA information systems. System Managers must monitor and document the training of information security personnel who support their systems to make sure they continually receive the necessary training to achieve the system's security and privacy objectives.

In addition, every FSA employee must receive annual information security awareness training that is adequate to fulfill his or her security responsibilities. Supervisors must monitor employee training, both type and frequency.

2.8 System Interconnections

FSA must have security control review of every system and interconnected systems on a periodic basis. FSA system owners must authorize all Memoranda of Understanding (MOU) or Memoranda of Agreement (MOA) between interconnected systems. Every system must have a network diagram and documentation of any interconnected systems including access to the Internet, its names/unique identifiers, and a description of the interaction(s) between or among them included within the System's Security Plan.

When obtaining system support or development services, FSA's contract agreements must include, but is not limited to,:

- How legal security and privacy requirements are met;
- Physical and logical controls to be used to restrict and limit access to sensitive information to only authorized users;
- The expected availability of services to be maintained in the event of a natural disaster or other interruption of normal processing; and
- Levels of physical security for outsourced equipment;
- FSA's right to audit;
- Security screening of contractor personnel and security training requirements for contractor personnel; and
- Language requiring a contractor to inform the FSA system manager and SSO when contract personnel depart from the contract.

3 OPERATIONAL CONTROLS

The System Operational Controls section addresses security controls that are implemented and executed by people as opposed to systems. These controls are put in place to improve the security of a particular system or group of systems. They often require technical or specialized expertise and rely on management activities as well as technical controls.

3.1 Personnel Security

FSA information security depends heavily on individuals, and the controls placed on the individual. Each user must adhere to standards of conduct that protect the confidentiality, integrity and availability of information networks and the data they contain, transmit or process.

System Managers are responsible for implementing and validating reasonable and prudent personnel security controls to protect the confidentiality and integrity of the data and/or information maintained by FSA, and to protect the availability of the networks that maintain, process or transmit that data and/or information. These controls are intended to assure the trustworthiness of all individuals who are allowed to access FSA networks. This process has several vital components, which include:

- Requesting, establishing, issuing, and closing user accounts,
- Documenting duties in a position description,
- Determining the sensitivity/risk level of each position,
- Establishing background screening commensurate with access level sensitivity and Departmental requirements,
- Use of external connections or transportable computers,
- Use of confidentiality agreements,
- Segregation of duties, and
- Assuring compliance with the process.

3.1.1 Establishing and Terminating Accounts

SSO's must use a documented process for requesting, establishing, issuing, and closing all user accounts. This process must include linkages to the human resource and contracting functions involved in new hires, transfers, contract award, oversight, and termination of employment. All user accounts must be regularly reviewed and kept current.

The SSO, or designee, must identify any system privileges or features, which would allow a user to override system or application controls, and associate these privileges with the categories of staff that would use them. SSOs must maintain an authorization process and record of privileges. SSOs must review authorization for privileged access rights at least quarterly to see if privileged access is still required, and to make sure users have not been erroneously assigned unauthorized privileges.

3.1.2 Position Descriptions

System Managers must establish job descriptions that accurately document assigned duties and responsibilities. The system manager must use these job descriptions when designating the sensitivity levels of these positions.

3.1.3 Sensitivity/Risk Levels

System Managers must classify the sensitivity of each position. When determining a position's sensitivity, consideration must be given to the laws, regulations, and policies that establish specific requirements for the protection of data and information an individual may affect (e.g. the Privacy Act and the Financial Services Modernization Act, referred to as the Gramm-Leach-Bliley Act).

3.1.4 Background Screening

Each FSA employee or contractor must undergo an appropriate background screening for his or her assigned positions prior to obtaining access to FSA systems. The amount of screening directly relates to the sensitivity level of the particular job position (see Handbook 11 for implementation procedures). Additionally, if an employee or contractor's position changes, FSA must update the background screening commensurate with the position. Screenings, both clearances and investigations, must be renewed at least every five years thereafter. This policy applies to all new and re-hired employees, as well as all contractors, subcontractors and consultants.

Every system must have documentation that describes the conditions for access to that system, especially when it is necessary to grant access prior to the completion of a background screening. The documentation also must state the compensating controls (e.g. accompanying an individual in a sensitive area) that will be used to mitigate associated risk.

FSA must follow the Department's established procedures describing how to conduct background screenings during the hiring or transfer of FSA employees and/or contractors, as well as documentation requirements.

3.1.5 Use of External Connections

When appropriate, terms and conditions of employment must state that security responsibilities extend outside of the workplace (e.g. telecommuting, travel, etc). FSA System Managers must approve all external connections in advance, and comply with FSA security standards. Individuals in possession of portable computers or storage media containing sensitive FSA information must not leave such equipment unattended at any time unless the information has been properly safeguarded. Such individuals take full responsibility and accountability for the equipment and the data it contains. The Department's policies on transportable computing devices govern the use of laptops, two-way messaging devices, pagers, etc.

3.1.6 Nondisclosure and Confidentiality Agreements

All FSA employees and contractors that access sensitive information must sign a nondisclosure and/or confidentiality agreement covering the privileged/sensitive data or

information with which they will come in contact by accessing FSA networks. Statutes, regulations and internal FSA policy define the data or information to be covered under such agreements. The annual Information Security Awareness Briefings must reemphasize the nondisclosure and confidentiality agreements.

3.1.7 Segregation of Duties

System Managers must create formal procedures defining the authority granted to each user or class of users. Users must only receive the minimum access(es) necessary to perform their jobs. FSA must separate system support functions to avoid allowing a single individual to perform multiple sensitive processes. Whenever possible, development, test and operational facilities must be separated to support this segregation of duties and prevent unwanted alteration or modification of operational systems. At least two persons must possess expertise in every important computer, network or telecommunications related areas. Key personnel must take regularly scheduled vacations and periodically rotate job/shift responsibilities. Having back-up expertise prevents undue interruptions in a system's service and also increases the likelihood that unauthorized or abusive acts will be detected.

3.1.8 Compliance

On at least an annual basis, System Managers must validate compliance with personnel security controls for all personnel under their supervision.

3.2 Physical and Environmental Protection

Physical and environmental security measures must protect FSA's systems, buildings, and related supporting infrastructures against any physical threats. Therefore, FSA must implement adequate physical security controls commensurate with the risks of physical damage or access.

3.2.1 Physical Access Controls

FSA must control access to facilities and rooms that house systems through the use of guards, identification badges, and/or entry devices such as keycards to prevent unauthorized entry. FSA must establish emergency exit and reentry procedures to protect assets during an emergency and to prevent unauthorized reentry into facilities after the emergency expires. FSA facility personnel must securely store unused keys, keycards or other entry devices used to enter sensitive areas and return these devices when no longer needed.

All FSA personnel must obtain and display their FSA identification badges at all times, regardless of the area's sensitivity. Facility personnel must authenticate visitors, contractors, and maintenance personnel through the use of preplanned appointments and identification checks, and must escort these persons when in restricted or sensitive areas.

Restricted or sensitive areas must have clearly defined security perimeters, with appropriate access controls. FSA must restrict access to these areas to authorized personnel only and grant access in a way that creates an audit trail. Audit logs must be reviewed periodically for suspicious activity. If applicable, facility personnel must

change entry codes periodically. FSA management and supervisors must regularly review the list of persons with physical access to these areas. FSA personnel must report and investigate all suspicious activity and/or security violations.

To protect data from unauthorized disclosure, FSA personnel and contractors must locate computer monitors displaying sensitive data in areas that prevent viewing by unauthorized personnel. Facility personnel must restrict and monitor physical access to data and telecommunication transmission lines and their housing facilities. In the case of portable/mobile devices, personnel must encrypt data files that contain information designated as "sensitive".

3.2.2 Environmental Controls

To protect FSA's supporting utilities, such as electric power distribution nodes and lines, heating/air conditioning facilities and units, water pipes, etc. FSA must maintain and periodically review its environmental assets for risk of failure. In particular, FSA must locate water circulation systems and piping in such a way as to prevent them from representing an environmental risk to critical electrical and/or data processing facilities. Facility personnel must implement controls to mitigate natural disasters (floods, earthquakes, tornadoes, etc.) as well as man-made disasters such as fire, water-line breaks, sewage problems, etc. Since power outages/spikes occur more frequently than most other utility problems, facilities must provide uninterruptible power supplies or backup generators to areas that support sensitive and vital FSA systems to allow critical systems to shut down without damage or loss of data. Where feasible, facilities must have alternate environmental controls, such as power sources, redundant air conditioning, etc. to maintain the functionality of critical data systems.

3.3 Production Input/Output Controls

All FSA systems must have procedures controlling system production inputs and outputs. Every FSA system user must have access to a help desk or other user support system capable of providing assistance to authorized users of the system in the event of an input/output incident.

FSA must ensure that unauthorized individuals cannot read, copy, alter or remove any printed or electronic information for their own use or the use of another. Only authorized users may pick up, receive, or deliver input and output information and media. To assist in compliance, FSA must externally label all media for sensitivity and include any special handling instructions on the label.

FSA System Managers must establish procedures and protection controls to safeguard the storage of media. Movement of sensitive media fromor into storage or restricted areas must be logged and an audit trail must be maintained to record all such movements. Security personnel must establish and maintain controls for transporting or mailing media or printed output.

FSA must establish procedures for shredding or destroying sensitive hardcopy media when no longer needed or when damaged/spoiled. These procedures must include a

logging form to keep track of the destruction. Every system also must have procedures for sanitizing FSA electronic media for reuse, storage or destruction when no longer needed or if it becomes damaged/spoiled.

3.4 Contingency Planning

FSA's Contingency Plan policy defines the emergency operating procedures that must be followed to make sure FSA's critical functions continue to operate and support IT systems in the event of disruptions, both large and small. Emergency procedures must have timelines for recovery and restoration of specified services prioritized by the system's mission criticality. FSA must regularly review and test backup and restoration procedures.

FSA must identify, prioritize and document its most critical and sensitive functions and operations, and the information system resources that support those functions. Thereafter, FSA must assess the changes to the processing priorities for each system and obtain approval by the System Manager with system owner input.

FSA must make sure that a comprehensive contingency and disaster recovery plan is in place and tested for each system on the basis of this prioritization. These plans must have detailed procedures for restoring operation of the system, including the personnel responsible and the timeline within which the FSA system must be returned to normal business operations. For systems restored from original software, system administrators must reset all system defaults. FSA must train personnel responsible to execute contingency procedures on FSA systems.

SSO's for new FSA systems must complete a comprehensive contingency plan prior to authorizing a system for processing. An existing system, when preparing for reauthorization, also must have a comprehensive contingency plan before granting authorization for processing. All contingency plans must incorporate the results of the latest Risk Assessments to focus attention on the likeliest disrupting events. SSOs must distribute the contingency plan to appropriate personnel.

3.4.1 Plan Maintenance

Each contingency plan must specify conditions necessary for activating the plan and who is to be involved in the activation decision. The system manager, SSO, and CSO must review and approve the contingency plan. In addition to the primary operating location, FSA must store plans at a secure offsite facility along with all necessary documentation for operating and/or restoring each of FSA's systems and applications. Additionally, FSA must maintain copies of key vendor contracts that impact the operation or restoration of core FSA functions at this location.

At least annually, System Managers must conduct and document tests of their contingency/disaster recovery plans. System Managers must readjust and update contingency and disaster recovery plans as necessary to continue their effectiveness. The

system manager must inform the Designated Accrediting Authority (DAA) of the results of the testing and any resulting readjustments to the plans.

3.4.2 Alternate Site Capability

FSA System Managers supporting FSA General Support Systems or Major Applications must plan for the use of a secure alternate processing site geographically removed from its primary site. Such alternate processing sites may only operate with a contract or service level agreement in place that includes the appropriate standards of confidentiality, integrity and availability.

3.4.3 System Backup

Every system must have documented backup procedures, which include frequency (daily, weekly, monthly) and scope (full backup, incremental backup, and/or differential backup). System operators must backup all systems' critical data files nightly and move the files to a geographically separate location each day. System personnel must ensure that all essential business information and software can be recovered up to the most recent system backup preceding any contingency event. System backups must be completed at least weekly. More frequent backups are required for critical systems or processes whose data is updated frequently. At least three generations/cycles of backup information must be retained for mission critical or mission important systems

3.5 Data Integrity

It is the responsibility of FSA System Managers to maintain the controls necessary to protect the integrity of data and information processed within their systems. Each FSA system manager must document data integrity procedures to describe how the system detects and prevents any unauthorized alteration or destruction of data, caused by either malicious or accidental means.

3.5.1 Virus Detection and Elimination

FSA must install virus detection and elimination software on every system. Once installed, System Managers must establish procedures for routine updates to virus signature files, including automatic and/or manual virus scans. Users must scan untrusted removable media. Virus scanning must include screening non-text files.

3.5.2 Verification

FSA systems must use integrity verification programs that meet the integrity requirements of the system. Such verification programs must look for evidence of deliberate acts such as data tampering, as well as data entry errors, corruption of correctly entered data and omissions. Techniques must include consistency and reasonableness checks and validation during data entry and processing.

3.5.3 Reconciliation

Every system must establish procedures to reconcile data transfers, including a description of the actions taken to resolve any discrepancies.

3.5.4 Message Authentication

FSA systems with requirements for non-repudiation and medium or high integrity must have written procedures on the use of message authentication. Message authentication is used both to verify identity of the sender of a message and determine whether or not the message has been altered during transmission. FSA personnel must review these procedures at least annually to sustain their continued validity.

3.5.5 Performance Measurements

Every system must use system performance monitoring to create and analyze system performance logs for availability problems, including active attacks and system and network slowdowns and crashes. Commensurate with the system's availability requirements, personnel may need to analyze performance logs on a near real-time basis. FSA System Managers must establish written procedures if their system requires near real-time performance analysis. System Managers also must identify whether their system's availability level can operate using periodic performance sampling or other less demanding controls. FSA System Managers must review these procedures at least annually.

3.5.6 Intrusion Detection

FSA System Managers must monitor current status of intrusion detection tools on the information systems and networks for which they are responsible. FSA systems' personnel must inform the system's owner whenever intrusion detection tools are implemented or modified. The records must include a description of intrusion detection tools installed on the system, where they are placed, the type of processes detected/reported, and the handling procedures. System logs must be reviewed for anomalies on a daily basis, using automated or manual methods. Additionally, FSA system mangers must routinely review intrusion detection reports after suspected incidents, and assign responsibility for incident resolution and lessons learned.

In order to validate intrusion detection tools, FSA System Managers must conduct periodic reviews on the software and data content of the systems for which they are responsible. All unapproved files or amendments discovered during such reviews are subject to a formal review process to determine the level of risk such unapproved software/data content represents, and the extent to which intrusion detection or other tools may not have performed adequately to alert system operators to the unauthorized installation(s). FSA must maintain formal documentation concerning all such reviews.

3.5.7 Penetration Testing

FSA System Managers must oversee the penetration testing performed on the system(s) for which they are responsible. In addition, they must establish procedures for each system to ensure that the penetration testing is conducted appropriately and on a periodic basis. The SSO must record results of such testing and report on the ensuing corrective actions.

3.6 Documentation

Every FSA system must have sufficient security documentation to describe adequately the security controls and procedures governing the operation and maintenance of the system. At a minimum, FSA System Managers must maintain the following documentation for all FSA Major Applications and General Support Systems:

- A current System Security Plan
- Certification and Accreditation documents and statements authorizing a system to process, including all required appendices.
- A log of service packs, patches upgrades, etc. for the system, and the order of installation.
- A Network diagram and documentation on placement and configuration of firewalls, intrusion detection sensors or other security software or appliances.
- Standard operating procedures that support all operations of the application or general support system.
- User manuals to explain correct usage of software/hardware.
- Vendor-supplied documentation of software and hardware.
- Application documentation, requirements, and specifications per the system's current contract.
- Software and hardware testing procedures and results.

The System Security Officer must know the locations and latest version numbers of all required documentation.

3.7 Configuration Management

Every FSA system manager must create a configuration management plan that describes the hardware and system software maintenance controls in place and the process by which configuration controls will be maintained for that system.

This must include an established, systematic process for addressing the introduction of new configurations into FSA systems and networks to make sure software upgrades or security patches work in the intended way and do not adversely impact other security or functionality aspects of the system. Therefore, all FSA systems must have the following configuration change controls in place.

3.7.1 Configuration Control

FSA System Managers must establish procedures to address configuration changes unique to the system. FSA must create a formal change control process for each system requiring tests and approval for any change before entering into production. The procedures must include the following:

- Every system must use software change request forms to document requests and related approvals.
- Every system must use version control, allowing association of system components to the appropriate system version.

- System security officers must attend the configuration control meetings and make recommendations on proposed changes.

3.7.1.1 Change Management

Each FSA system manager must make sure every system for which he/she has responsibility follows the configuration management process, including descriptions and enforcement of change identification, approval, and documentation procedures. Each FSA system manager must make recommendations on the required training needed for both technical and user communities to implement new configurations and controls.

FSA change management processes must include the following:

- Impact Analysis to determine the affect of proposed changes on existing security controls, including the required training needed to implement the control.
- Documentation of all changes to application software along with the procedures used for testing and/or approving changes to system components prior to proceeding to the production environment.
- Specification of the type of test data to be used (live or made-up) in the testing process.
- If live data is to be used, specification of the process for assuring the confidentiality and integrity of the data.
- Documentation of test results and, upon implementation, System Manager's review of the updated detailed system specifications.
- Documentation describing the distribution and implementation of new or revised software, including effective date for all locations.
- Consideration of special procedures for performance of emergency repair, emergency maintenance, and interim authorization for processing.
- Documentation of emergency change procedures, which must be approved by management within a maximum of five days. These procedures must be dynamic and regularly updated to draw upon actual experiences with emergencies.
- Updates to system security plans, contingency plan, and other associated documentation.

3.7.2 Configuration and Management Documentation

Every FSA system manager must develop procedures to restrict or control the activities of those who perform maintenance and repair activities, both on-site and off-site. These procedures must fully consider the criticality of the system and the need to protect the confidentiality, integrity and availability of the data and information it contains and/or processes. FSA System Managers must specify the procedures that reflect issues such as the escort of maintenance personnel, sanitization of devices removed from the site, and other issues relevant to the systems under his/her control. The SSO may document these procedures in a Configuration Management Plan and/or in the system's security plan

3.7.2.1 Maintenance and Repair

FSA System Managers must review all default security parameters to correlate with system sensitivity requirements. In most instances, default security settings should be set to a restrictive setting. Where necessary, use the most restrictive settings.

Every system manager must describe procedures used to control remote maintenance services. FSA System Managers must implement access controls and other security precautions to prevent potentially malicious code, such as "back doors," from being used to evade authentication and authorization protections. Implementation of maintenance or repairs must take place at such times and under such circumstances so as to minimize impacts to business processes.

System Managers periodically must review their systems to identify and, when possible, eliminate unnecessary services (e.g. FTP, HTTP, mainframe supervisor calls). Additionally, System Managers periodically must review their systems for known vulnerabilities and current installation of software patches.

3.7.2.2 Unapproved Software

Software installation and use must follow the principle that whatever is not expressly allowed is denied. FSA must establish organizational procedures for dealing with, and protecting against, the inappropriate use of copyrighted software. If FSA uses a copyrighted product, sufficient licensed copies of the software must be purchased for each system on which the application will be processed.

In the unusual instance where personally owned software/equipment is used for processing FSA business, the user must document each instance including provisions to protect software copyrights and inform their supervisor in writing. The Department must perform periodic audits of FSA computers to make sure users do not install unapproved software.

3.7.2.3 Application Ownership

Contracts must clearly specify whether the government owns the software, whether the software was developed in-house or under contract, or if the application software was received from another federal agency with the understanding that it was federal government property.

3.8 Incident Response

The confidentiality, integrity and availability of FSA networked systems will depend in part on the preventative security measures to deter or inhibit attacks. FSA must employ intrusion detection tools, firewalls, automated audit logs, and other preventative measures to assist system security staff when a security incident occurs in a system.

FSA must adequately train system security personnel to recognize security incidents. FSA must establish procedures for reporting and responding to those incidents. Once identified, FSA must monitor and track an incident until resolved, and maintain documentation concerning the incident and its resolution.

3.8.1 Information Sharing

FSA must share information regarding incidents and common vulnerabilities or threats with FSA system personnel and appropriate managers of systems and networks interconnected with FSA.

FSA management must assign specific individual(s) to receive and respond to alerts/advisories, vendor patches, exploited vulnerabilities, etc.

3.8.2 Incident Identification

FSA adequately must train system security personnel to recognize security incidents. Non-security personnel must never attempt to prove suspected weaknesses on their own, as FSA must treat this act as an actual attack that may result in heavy penalties, including termination of employment.

Users must notify FSA System Managers and/or system administrators as soon as possible about any observed or suspected security weaknesses in, or threats to, FSA systems or services. Once reported, FSA must analyze security alerts and security incidents and take appropriate actions. Users must report software malfunctions and report the malfunction using the same procedures.

The SSO must report incidents to the CSO. The CSO will forward these reports to ED O/CIO for further dissemination.

3.8.3 Post Incident Activities

FSA System Managers must review incident handling procedures and control techniques after each incident and, when necessary, modify the procedures to prevent recurrence. In addition, FSA System Managers must collect and secure audit trails and other tracking mechanisms for analysis and use as potential evidence.

4 TECHNICAL CONTROLS

The System Technical Controls section focuses on security controls that the system executes as opposed to controls executed by people. These controls depend on the proper functioning of the system for their effectiveness.

4.1 Identification and Authentication

Each FSA system must use identification and authentication procedures to prevent unauthorized use or access. Before granting initial access to an FSA system, SSO's must verify the following:

- The user has authorization from the system owner to access the system,
- The level of access is appropriate for the user's business purpose,
- The access will not compromise segregation of duties,
- The user received a copy of the Rules of Behavior for the system and has signed a statement indicating that he/she understands and agrees to the Rules, and
- Completion (for high-risk positions) or initiation (for low-medium risk positions of proper background screening.

FSA systems must correlate actions to users via the creation of unique user IDs for each individual user. These IDs must not give any indication of a user's privilege level (i.e., Administrator, etc.). System owners must permit and approve Group IDs only when necessary. Any user who requires special privileges or features beyond their primary job function, which would allow them to override system or application controls, must use an additional user ID different than that used for normal business purposes. Along with user IDs, FSA systems must have documentation describing whether passwords, tokens, biometrics or other methods are used for access purposes and how the access control mechanisms will support individual accountability and audit trails. At a minimum, these access control methods should be associated with the unique user IDs.

Security controls must be able to detect unauthorized and/or invalid attempts to access FSA systems. The number of invalid access attempts that may occur for a given user ID or access location (i.e. terminal or port) must be determined and documented. Within the documentation, the SSO must include the actions taken when that limit is exceeded.

When an FSA system allows bypassing of user authentication requirements, (for example, single-sign-on technologies, host-to-host authentication servers, user-to-host identifier, and group user identifiers), the SSO must document the governing procedures, as well as any compensating controls and whether emergency or temporary access is authorized. Host-based authentication, granting access based on the identity of the host originating the request instead of the individual user requesting access, is permitted to control access. If this method is used on FSA systems, it must be documented and controls put in place to remove access authorization when hosts no longer have legitimate access.

4.1.1 System Login

Login procedures must include an appropriate banner containing the following warning:

You are about to access a United States government computer network intended for authorized users only. You should have no expectation of privacy in your use of this network. Use of this network constitutes consent to monitoring, retrieval, and disclosure of any information stored within the network for any purpose including criminal prosecution.

The banner must include a "click through" requirement so that the person logging in must agree to the terms before accessing the FSA system.

Login procedures must also limit the amount of information displayed about the system and its functions until after a user has successfully logged in. FSA systems must not display the following during login:

- System or application identifiers,
- Help messages, and
- Validation of any portion of the login information, for example, not indicating which part of the login data was correct or incorrect.

In addition, FSA systems' logins must mask a user's password during login.

4.1.2 Passwords

If passwords are the access control method used for authentication to an FSA system, SSOs must document password procedures for each system. The documentation must include specific information regarding allowable character sets, password length (maximums and minimums), password aging time frames and enforcement approach, and the number of generations of expired passwords disallowed for use. Acceptable FSA passwords must contain a minimum of eight characters in length and include any combination of the following to meet or exceed FIPS Publication 112 standards:

- English uppercase letters (A-Z)
- English lowercase letters (a-z)
- Westernized Arabic numerals (0-9)
- Non-alphanumeric special characters (!, @, #, $, &, *)

Any vender-supplied and/or default passwords on FSA systems must be changed immediately. If users maintain their own passwords, an initial password will be distributed to the user in a secure manner. Immediately upon initial login, the user will be forced to change their password. Temporary passwords (if a user forgets their password) must only be given after positively identifying the user. The temporary password must also be distributed to the user in a secure manner, and users must change it immediately upon initial login. Users will be informed not to write down or reveal their passwords to anyone. Procedures must be in place for handling lost and/or compromised passwords. Any password transmissions or storage will be encrypted to prevent capture.

Procedures must be in place describing creation of emergency passwords. These procedures must include who may authorize, duration of password validity, and criteria for granting emergency access.

Users must change their passwords at least every ninety days or earlier if needed. Every system must establish procedures to enforce password changes and identify who changes their passwords. To determine if user passwords meet the minimum standard, FSA must establish procedures (such as using password crackers/checkers) to determine compliance. Use of such tools must be limited to only those persons expressly authorized by the system manager. The system manager must record the authorization and specify the locations, systems and duration covered by the authorization.

Every FSA system must have procedures that describe how it limits access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, or scripts with embedded passwords are allowed only for specific (i.e. batch, etc.) applications).

4.1.3 PKI and Biometrics

FSA or FSA contractor's use of Public Key Infrastructure (PKI) technology must conform to FIPS 186-2, Digital Signature Standard, and FIPS 180-1, Secure Hash Standard, issued by NIST, unless the system manager grants a waiver. If granted, the system manager must include the name and title of the official granting the waiver. Every system must have procedures describing cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction, and archiving.

Documentation for every FSA system must describe whether encryption is used to prevent unauthorized access to sensitive data transfers. If PKI is used, the system manager must create procedures detailing how PKI certificates are generated and controlled. If encryption is used primarily for authentication, the SSO must include this information in the encryption documentation.

Biometrics and/or tokens are permitted as other access control methods to authenticate users to their systems. Systems using these methods must describe the controls used and how they are implemented on the system. Documentation must indicate if any special hardware (such as card readers) is required, if users are required to use a unique Personal Identification Number (PIN), and who selects the PIN.

4.2 Logical Access Controls (Authorization/Access Controls)

FSA's logical access security controls are system-based mechanisms that must restrict users to authorized transactions and functions only. These controls must detect unauthorized transaction attempts by authorized and unauthorized users and must reside at the application, operating system, and/or network level, depending on the system.

Access controls for FSA systems and networks must:

- Deny access to systems by undefined users or anonymous accounts,

- Limit and monitor the usage of administrator and other powerful accounts,
- Suspend or delay access capability after a specific number of unsuccessful logon attempts,
- Disconnect automatically at the end of a session,
- Remove obsolete user accounts as soon as an employee leaves FSA,
- Suspend inactive accounts after 90 days,
- Remove redundant user IDs, accounts, and role-based accounts from resource access lists,
- Protect Audit Logs through strict access controls, and
- Protect the confidentiality of sensitive information during data transfers and storage.

Every FSA system must have documentation that describes the specific security controls for hardware and software features that are designed to permit only authorized access to or within an application, its data, or other files. In addition, every FSA system must have documentation that describes any restrictions to prevent users from accessing the system or its applications outside of normal work hours or on weekends. FSA System Managers must establish procedures to restrict and control access to all program libraries, system software, and system hardware. Access to security software and hardware is restricted to security administrators. Any privileges allowing a user to override these system or application security controls may only be granted to individual users when it is determined that the user needs these privileges to perform his or her job. When granted, such privileges must be at the minimum level necessary to complete the specific job.

FSA System Managers must assign a person(s) to review protocols with known vulnerabilities, such as UDP and TFTP, and grant approval for their use prior to implementation. Documentation for every system must describe any type of secure gateway or firewall in use, including its configuration. If installed, firewalls must meet the standards set forth in the FSA Enterprise Technical Architecture document. System personnel must disable unused system features, services, protocols and ports. System personnel must also reinitialize all vendor supplied default security parameters to more secure settings. Documentation regarding any port protection devices requiring specific access authorization to the communication ports must include the configuration of the port protection devices and whether additional passwords or tokens are required.

4.2.1 Access Control List

FSA System Managers must assign an employee to create and maintain a current list of authorized users and their access. The system manager must approve the list before its implementation. This Access Control List (ACL) must be protected to prevent unauthorized access or viewing of the file. The person(s) responsible for the ACL must remove users who no longer have access rights from the ACL. To corroborate this process, system personnel must review ACLs at least every six months to identify and remove users who have left the organization (inactive users), users whose duties no longer require access to the application or system, invalid users, and redundant user IDs and accounts.

4.2.2 Internet or Public Access

If an application is running on an FSA system that is connected to the Internet or other WAN, FSA must install additional technical security controls to provide protection against unauthorized system penetration. Authorization procedures must determine which network and network services are allowed and who is authorized to access them.

If the public accesses an FSA system, FSA must develop and implement security controls to protect the integrity of the application and the confidence of the public. Each FSA web page must have a designated author or administrator who is responsible for ensuring web page security. If a server contains information protected by the Privacy Act, it must not be accessible without proper authorization. Additionally, the website should provide notice that it contains Privacy Act information, and give notice of the consequences of unauthorized disclosure. Users wishing to access internal FSA systems via the Internet must be authenticated.

4.2.3 Remote Access

An FSA user may only be authorized to telecommute (i.e., dial-in, VPN, etc.) after he/she has submitted a request to the system manager, and the system manager and SSO for the system have reviewed and accepted the request. Appropriate system personnel must monitor all dial-in access.

4.3 Audit Trails

FSA audit trail records must maintain a log of system and network activity both by system or application processes and by user activity for a minimum of one year. In conjunction with appropriate tools and procedures, audit trails must provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems. These tools will assist system managers to investigate suspicious activity and take appropriate actions.

FSA must strictly control and protect access to audit logs and automated tools against unauthorized changes and/or operational problems. This is especially necessary if anyone can review the logs online and/or if they contain personal information about FSA users. To access and review audit logs, the reviewer must be an appropriate system-level or application-level administrator. Logs must be reviewed after a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem. The use of automated tools is recommended to help interpret information contained in audit records, discard irrelevant or mundane task information, as well as to distill useful information from the raw data.

FSA audit logs must include:

- Information on all activity involving access to and modification of sensitive or critical files.
- Sufficient information to establish what events occurred, and who or what caused them. In general, an event record must specify:
    - Type of event;

    - When the event occurred;
    - User ID associated with the event; and
    - Program or command used to initiate the event.
- Records of the number of successful and rejected system access attempts, data access attempts, and other resource access attempts.

The audit logs must have the capability of being queried by user ID, terminal ID, application name, date and time, or some other set of parameters in order to run reports of selected information. Audit trail clocks must be synchronized to an agreed upon standard to avoid discrediting the validity of the logs during an investigation. FSA System Managers must develop procedures to check and correct any deviations in the time.

Whenever FSA uses keystroke monitoring, the SSO must document the procedures and provide a means of user notification. Also, the procedures must indicate whether the Department of Justice has reviewed the policy.

FSA must segregate the duties between FSA security personnel who administer the access control functions and those who administer audit functions. This is to protect audit functions and/or access control functions from being intentionally or unintentionally reconfigured.

Appendix A - Roles and Responsibilities

Position Title	Roles and Responsibilities
FSA Chief Operating Officer (COO) – Responsible for protecting IT resources within FSA, establishing policy and directives, and directing implementation of security practices.	❑ **Accept** overall responsibility for securing FSA data and information systems. ❑ **Accept** overall responsibility for establishing and reviewing FSA security and privacy policy ❑ **Appoint** a Computer Security Officer (CSO) ❑ **Encourage** Department of Education and extra-Departmental (GAO, OMB, etc.) participation in FSA security and privacy matters ❑ **Review** certification recommendation and grant systems the authority to operate
Computer Security Officer (CSO) – Implements and maintains the Information Technology Security Program within FSA. Advises FSA Management Council. Coordinates security policy and directives and supports the SSOs. Works closely with Department of Education security officials. The CSO also serves as security and privacy advisor to an FM. Works with SMs and SSOs to develop and implement security policy and procedures within a functional area. Stays current on security and privacy related events and keeps current on security training,	❑ **Review** Department of Education and government-wide information security and privacy policies and incorporate them into FSA policy ❑ **Appoint** primary points of contact for security incidents ❑ **Receive** and **act** on notifications of security and privacy incidents ❑ **Meet** regularly with Department and FSA security officials ❑ **Accept** overall responsibility for the FSA Security & Privacy website ❑ **Provide** security and privacy awareness training for FSA ❑ **Coordinate** responses to external requests for security information about FSA ❑ **Coordinate** risk assessments, independent (A-130) reviews and Certification and Accreditation with security managers ❑ **Maintain** and **review** the System Security Plan, Disaster Recovery Plan, Contingency Plan and Continuity of Operations Plans for each IT system within FSA ❑ **Make sure** physical security requirements are met for each FSA information technology installation and system ❑ **Establish** and **enforce** policies on introduction and removal of IT hardware/software into and from FSA systems and facilities (too detailed) ❑ **Provide advice and counsel** to the FM, SSOs and System Managers in all security and privacy matters ❑ **Review** current events, training notices, and changes to legislature, regulations or policy and help disseminate within the organization ❑ **Coordinate** with relevant SSOs to identify information security and privacy issues, define

	solutions, and monitor progress ❑ **Participate** in Departmental, FSA, industry and governmental security and privacy working groups ❑ **Work with FSA Personnel Security Officer to implement proper personnel security in staff and contractors** ❑ **Help develop** standard language and / or performance standards on security and privacy for FSA contracts
Functional Manager (FM) - Top-level FSA managers with one or more IT systems under their control. Includes General Managers, Ombudsman, CFO and CIO. Responsible for information systems within their respective areas, and for establishing, maintaining, and enforcing computer security policy.	❑ **Designate** a System Manager (SM) and System Security Officer (SSO) for each information system ❑ **Hold** SSOs and SMs accountable for assigned security duties ❑ In role as Data Owner, **Establish** data elements designated as sensitive information ❑ **Review** future development efforts with the CSO, SM, and SSO to make sure security is handled in a consistent manner across FSA, and complies with Departmental and government-wide security and privacy requirements
System Manager (SM) – Designated by the FM. Supervises the daily operation and maintenance of a specific information system. Manages personnel, system operations, and interoperability with other systems. Coordinates the efforts of administrators (systems, network, and database), system maintenance personnel, and system programmers. Responsible for the accuracy, confidentiality and availability of the data in a specific information system. Only a data	❑ **Create** detailed position descriptions that define role-based system privileges ❑ **Create** a system-specific list of approved software ❑ **Establish** processes to protect the integrity of information contained and data passed from one person or system to another ❑ **Identify** system information exchanges and **assure compliance** with established exchange standards ❑ **Establish** specific training requirements for users and managers of the system ❑ **Make sure** all system development efforts are accomplished exclusively in a development environment that reflects the production environment, and tested with approved test data to reduce the risk of compromising data when new system components go live ❑ **Review** system risk assessments and risk mitigation strategies ❑ **Prepare** system certification and accreditation package for FM, brief FM and CSO on certification findings ❑ **Act** on reported security and privacy incidents by approving remedies and notifying FM and CSO

owner has authority to grant access to his / her data. In FSA, FMs are data owners for systems they control.	❑ **Make sure** configuration management policies are followed when making system or system environment changes ❑ **Make sure** system requirements include security and privacy guidelines ❑ **Make sure** contractors develop a System Security Plan, Disaster Recovery Plan, Contingency Plan, and Continuity of Operations Plan for the system and that plans are updated at least annually ❑ **Monitor** system availability by **reviewing** expected system event procedures, such as system start-up and initialization, system shut-down, database updates, and software changes
Contracting Officer's Representative (COR) -	❑ **Require** offeror to present a detailed outline of proposed information technology security program and document compliance with the FSA security requirements ❑ **Make sure** technical proposal instructions include a statement of security compliance requiring the offeror to comply with the security requirements identified in the statement of work. This clause must include 'flow-down coverage' to make sure all sub-contractors used to support the work effort will also meet the requirements identified in the clause. ❑ **Provide** applicable FSA security documents upon request
System Security Officer (SSO) - Designated by the SM or equivalent, the SSO implements FSA's security policy in a specific information system. Responsible for protection and privacy of information processed or stored in that system. Serves as the focal point for the physical security of the system.	❒ **Coordinate** with SM to determine appropriate security requirements for system ❒ **Make sure developers, operators and** users are informed and trained in security and privacy matters ❒ **Participate** in system risk assessments and support development of a risk mitigation strategy ❒ **Coordinate** requests for system access with the FSA Personnel Security Officer ❒ **Recommend** approval / disapproval for system changes based on the risk to the security and privacy of the system ❒ **Identify** the need for data protection where sensitive data are transmitted across open networks ❒ **Consider** security issues of any remote/dial-up facilities and the need to **protect** these facilities from unauthorized use ❒ **Review** and **recommend** changes to the system's Disaster Recovery Plan, Contingency Plan, Continuity of Operations Plan and System Security Plan ❒ **Advise** SM on identifying controlled areas ❒ **Make sure** necessary physical security is in place to protect system assets ❑ **Oversee creation** and **maintenance of** up-to-date user lists ❑ **Make sure there are no** guest accounts on FSA systems ❑ **Make sure** audit tools are used to track user activities on the system ❑ **Monitor** security events of the system and report anomalies to SM and CSO

	❑ **Document** expected system event procedures, such as system start-up and initialization, system shut-down, database updates, and software changes ❑ **Document** abnormal events, such as system failures, unsuccessful system initializations or shut-downs, system error responses, and corruption or loss of data ❑ Based on risk assessments, **make sure** the necessary security controls are updated in the System Security Plan ❑ **Support** the FM in identifying and developing security requirements for new systems and system enhancements ❑ **Review** all contracts **and subcontracts** for compliance with FSA security policy and assist the relevant business unit and the Contracting Officer with these efforts
System Administrator – Usually performed by contractor personnel. Responsible for implementation of system level security policy and procedures	❑ **Make sure** password procedures for assigned systems meet Federal and FSA standards ❑ **Make sure** personnel security clearances are complete and properly documented prior to issuing system access / password ❑ **Make sure** permissions granted are specific to the individual position and system role / responsibility ❑ **Identify** authorized users through the use of unique user IDs and passwords ❑ **Make sure** written system procedures are accurate and recommend changes to the SM ❑ **Implement** system logs and controls to allow for identifying, recording, reporting, and assigning accountability for activities that occur within an information system ❑ **Restrict** access to system utilities that may bypass or security controls ❑ **Restrict** users' ability to install any unauthorized software ❑ **Revoke** access to invalid or expired user accounts ❑ **Remove** guest accounts from FSA systems ❑ **Make sure** all system administration materials required to support the Disaster Recovery, Contingency and Continuity of Operations Plans are pre-staged at the designated safe location

Network Administrator - Usually performed by contractor personnel. Responsible for network level security of system database information security of system	❑ **Enforce** the use of database access methods, which incorporate data integrity checks ❑ **Review** Disaster Recovery, Contingency and Continuity of Operations Plans and recommend changes to the SM and SSO ❑ **Make sure** all database administration materials required to support the Disaster Recovery, Contingency and Continuity of Operations Plans are pre-staged at the designated safe location
Database Administrator Usually performed by contractor personnel. Responsible for database information security of system	❑ **Limit** direct database access to database administrators ❑ **Review** written system procedures for accuracy and recommend changes to SM ❑ **Implement** database logs to associate data changes with specific users ❑ **Enforce** the use of database access methods, which incorporate data integrity checks ❑ **Review** Disaster Recovery, Contingency and Continuity of Operations Plans and recommend changes to the SM and SSO ❑ **Make sure** all database administration materials required to support the Disaster Recovery, Contingency and Continuity of Operations Plans are pre-staged at the designated safe location
System Developer Usually performed by contractor personnel. Along with SSO, developer should ensure security is integrated into the solution, beginning with the Vision Phase of the Solution Lifecycle	❑ **Make sure** system documentation is updated to maintain currency with system changes ❑ **Follow** the Security Solution Lifecycle during the development and operation of the system ❑ **Implement** transaction assurance procedures, such as error detection and checksum comparisons, for data transfers between system resources ❑ **Test** newly developed software prior to moving into the production environment ❑ **Prohibit** developers from directly accessing production libraries, except where authorization is granted by the SM and SSO ❑ **Develop** test data for system testing, making sure operational data is not used during system testing ❑ **Notify** the network administrator of necessary network services that must be approved by the system manager